● PRINTER RUSH ●

(PTO ASSISTANCE)

Application :	09/775206	**Examiner :**	Sheikh	**GAU :**	2131
From:	T. McGill	**Location:**	(IDC) FMF FDC	**Date:**	12-23-04

Tracking #: 0021207 Week Date: 10-11-04

DOC CODE	DOC DATE	MISCELLANEOUS
☐ 1449		☐ Continuing Data
☐ IDS		☐ Foreign Priority
☒ CLM	8-12-04	☐ Document Legibility
☐ IIFW		☐ Fees
☐ SRFW		☐ Other
☐ DRW		
☐ OATH		
☐ 312		
☐ SPEC		

[RUSH] **MESSAGE:** Claim 23 depends on canceled Claim 22.

thank you

[XRUSH] **RESPONSE:**

(1) The claim 23 should now depend on Claim 18 instead of claim 22 due to the cancellation of claim 22.

(2) The "corrected" Detail Action of Allowance is attached (See page. 3, Item # 10 & 11).

INITIALS: LBC

2/14/2005

NOTE: This form will be included as part of the official USPTO record, with the Response document coded as XRUSH.

REV 10/04

DETAILED ACTION

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John Rogitz on 09/14/2004.

The application has been amended as follows:

1. Please replace claim 1 with the following:

2. A method for defining sets of encryption keys from a key matrix, comprising: receiving at least one parameter representing a characteristic of the key matrix; using the parameter and an error-correcting code, defining plural sets of keys; and assigning at least some sets of keys to at least some respective devices, wherein the receiving act includes receiving at least a row parameter "N" representing the number of rows in the key matrix and a column parameter "n" representing the number of columns in the key matrix, and the method further includes: using an error-correcting code having a Hamming distance "d" that minimizes key overlap between sets of keys.

3. Please cancel claim 4.

4. Please replace claim 5 with the following:

5. The method of claim 1, wherein the error-correcting code defines the sets of keys using a total predefined number "T" of sets.

6. Please cancel claim 13.

7. Please replace claim 18 with the following:

8. A computer programmed with instructions to cause the computer to execute method acts including: receiving, as input, at least a number "n" representing a number of columns in a key matrix and a number "N" representing a number of rows in the key matrix, each position in the key matrix being definable by a respective index, each index being associated with a respective key useful by a decryption device for decrypting encrypted content; defining, based at least in part on the input, plural sets of keys using a non-random function, wherein the error-correcting code is associated with a generating matrix G, and the method executed by the computer further comprises storing the generating matrix G and an index of a stored set of keys, whereby no set of keys other than the index of the stored set of keys need be stored in that sets of keys can be regenerated using the generating matrix G and the index of the stored set.

9. Please cancel claim 22.

10. Please replace claim 23 with the following:

11. The computer of claim 18, wherein the method executed by the computer further comprises transforming the generating matrix G to have a non-systematic row assignment.

12. Please replace claim 25 with the following:

13. The method of claim 1, wherein the error-correcting code is a linear code.

Priority

14. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows:

15. The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application); the disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

16. Therefore, the effective filing date for the subject matter defined in all of the claims in this application is 02/05/2001because the claimed beneficial priority date on 08/23/1999 is not granted.

Allowable Subject Matter

17. Claims 1 – 3, 5 – 12, 14 – 21, and 23 – 27 are allowed.

18. The following is an examiner's statement of reasons for allowance:

19. The closest cited prior art (U.S. Patent No. US 2003/0223579 A1) fails to teach or suggest the features of defining a plural sets of encryption keys based on error-correcting code for efficient key storage purpose so that a plural sets of keys can be regenerated solely from (a) the index of the stored set of keys and (b) the characteristic

generating matrix, and using the hamming distance d to minimize the overlaps between multiple sets of keys in view of the addition limitations recited by independent claims 1, 9 and 18 because prior-art only defines public keys based on error-correcting code in such a way that the code received can still be recovered from the errors that occur due to the public key corruptions even though all the operations required for encryption are performed by the corrupted public key.

20. Claims 2 – 3, 5 – 8, 10 – 12, 14 – 17, 19 – 21 and 23 – 27 would also be allowable for the reasons stated above

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC